US007305555B2

(12) **United States Patent**
Okimoto et al.

(10) **Patent No.: US 7,305,555 B2**
(45) **Date of Patent: Dec. 4, 2007**

(54) **SMART CARD MATING PROTOCOL**

(75) Inventors: **John I. Okimoto**, San Diego, CA (US); **Eric J. Sprunk**, Carlsbad, CA (US); **Lawrence W. Tang**, San Diego, CA (US); **Annie On-yee Chen**, Del Mar, CA (US); **Bridget Kimball**, Encinitas, CA (US); **Douglas Petty**, San Diego, CA (US)

(73) Assignee: **General Instrument Corporation**, Horsham, PA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 951 days.

(21) Appl. No.: **10/109,111**

(22) Filed: **Mar. 27, 2002**

(65) **Prior Publication Data**

US 2003/0188164 A1 Oct. 2, 2003

(51) **Int. Cl.**

H04L 9/00	(2006.01)
H04K 1/00	(2006.01)
G06F 11/30	(2006.01)
G06F 12/14	(2006.01)
G06Q 40/00	(2006.01)
H04L 9/32	(2006.01)
H04N 7/167	(2006.01)
H04N 1/44	(2006.01)
H04K 1/02	(2006.01)

(52) **U.S. Cl.** **713/168**; 713/177; 713/181; 713/170; 713/189; 713/165; 713/176; 713/169; 705/51; 705/52; 705/53; 705/54; 705/55; 705/56; 705/57; 380/232; 380/278; 380/281

(58) **Field of Classification Search** 380/201–284; 713/171–201, 165, 168–170; 705/51–57
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,604,801 A * 2/1997 Dolan et al. 713/159

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0471373 A2 2/1992

(Continued)

OTHER PUBLICATIONS

Schneier, "Applied Cryptography Second Edition: protocols, algorithms, and source code in C", Applied Cryptography, John Wiley & Sons, New York, pp. 30-31, 180-181, 265-301, 351-354, 429-459, XP002104180.

(Continued)

Primary Examiner—Ayaz Sheikh
Assistant Examiner—Shin-Hon Chen
(74) *Attorney, Agent, or Firm*—Larry T. Cullen

(57) **ABSTRACT**

A system is described for uniquely mating components of a communication network such as a smartcard and a set-top box. When mated, the smartcard and set-top box are tied together and have a single identity. Further, the smartcard operates properly only when inserted into an authorized set-top box. Exchanges of information between both components are secured by encryption and authentication to guard against piracy of the exchanged information. The system provides the same authentication key to the set-top box and the smartcard. This key is used for authenticating communication between the set-top box and the smartcard. First, the authentication key is encrypted by a set-top box mating key. The set-top box employs this mating key to decrypt the authentication key. After it is derived, the authentication key is stored in the set-top box's memory. Further, the same authentication key is encrypted by a smartcard mating key. Thereafter, the smartcard employs the smartcard mating key to extract the authentication key. The clear authentication key is stored in the smartcard's memory as well. In this manner, the authentication key is used for securing all communication between the set-top box and the smart-card. For example, the set-top box may request control words from the smartcard. Only after authenticating the request, are the control words for decrypting digital content provided to the set-top box. If the smartcard authentication key is different from the set-top box key, the request for control words is denied.

17 Claims, 6 Drawing Sheets